SSS:JV
F.#2019R01298

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF WHITE APPLE IPHONE X, CURRENTLY WITHIN THE AFFIANT'S POSSESSION IN THE EASTERN DISTRICT OF NEW YORK	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 19-MJ-982

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, ROBERT T. CARASITI, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been a Special Agent with the FBI for five years and am presently assigned to the John F. Kennedy International Airport ("JFK Airport") Resident Agency in New York. I have been involved in the investigation of numerous cases, mostly involving terrorism. As part of those investigations, I have made arrests, interrogated subjects, collected evidence and interviewed witnesses. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file, including the defendant's criminal history record; and reports from, and conversations with, other law enforcement officers

involved in the investigation. I have received training generally concerning searches of electronic devices.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a white Apple iPhone X belonging to Emmanuel Asuquo Okon (the "Device"). The Device is currently in my possession within the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On or about September 24, 2019, a security company (the "Victim Security Company") transported in an armored vehicle eight bags, which contained cash in United States and foreign currency, from a facility at JFK Airport in Queens, New York. Employees of a separate company authorized to operate at JFK Airport brought the eight bags to a Delta aircraft located at Gate C-70. They were escorted by security. There, Quincy Thorpe, an employee of Delta Ground Services ("DGS"), scanned and loaded bags into Delta Flight 1225, bound for Miami, Florida ("Flight 1225"). Once Flight 1225 arrived in Miami, the Victim Security Company realized that one of the eight bags, which itself contained smaller bags, was missing (the "Stolen Bag"). According to the Victim Security Company, which had custody over the Stolen Bag, the Stolen Bag contained cash of approximately $258,205 in value.

7. Security surveillance obtained from Delta shows an individual consistent with the appearance of Thorpe scanning and loading some of the eight bags onto Flight 1225. Other

DGS employees stated in sum and substance and in part that Thorpe was responsible for loading bags onto Flight 1225. Additionally, the other seven bags, which were loaded onto the plane, were scanned by a scanner with an identification unique to Thorpe.

8. Security surveillance shows Thorpe not scanning the Stolen Bag, but instead placing it into a container attached to a vehicle. Specifically, Thorpe placed the Stolen Bag into a luggage trailer attached to a vehicle (the "Tug and Trailer"). After loading some of the bags onto Flight 1225, Thorpe drove the Tug and Trailer to a Terminal 2 underground entrance, where he left the vehicle. Security surveillance shows that, at that time, the Trailer curtain was closed.

9. Security surveillance also shows that, while at the Terminal 2 underground entrance, Thorpe was using a cell phone. Shortly thereafter, a Delta van pulled up to the Terminal 2 underground entrance and Thorpe walked over and spoke to the van driver through the passenger side window. After speaking to the Delta van driver, the van pulled away. Thorpe then re-entered the Tug and Trailer and also pulled away from the Terminal 2 underground entrance.

10. Both the Delta van and the Tug and Trailer then traveled to the same remote area of the airport where they stopped briefly behind a parked aircraft. Less than one minute later, both vehicles left the remote area and returned directly to the same Terminal 2 underground entrance. When they arrived back at the Terminal 2 underground entrance, the previously closed side of the Trailer was open and empty. I believe that Thorpe traveled with both the Tug and Trailer and the Delta van to the remote area so that he could move the Stolen Bag from the Tug and Trailer into the Delta van away from security surveillance.

11. After returning the Tug and Trailer to the Terminal 2 underground entrance, Thorpe left the vehicle and entered the Delta van. The Delta van then left the airport secured

area of operations and proceeded to another unsecured area of the airport, specifically to a parking lot behind Building 21. The Delta van driver told law enforcement that Thorpe spent most of the ride on the phone speaking to someone named "Okon," and directing "Okon" to their location.

12. Between 9 and 9:30 a.m., and approximately 11 minutes after the Delta van arrived in the parking lot, a blue Nissan Sentra arrived and pulled up behind the van. Security surveillance shows that the driver of the blue Nissan Sentra was a black male with a beard, which is consistent with the appearance of Emmanuel Asuquo Okon. In addition, a witness has identified the Sentra driver as Okon.

13. Approximately two minutes after the Sentra arrived at Building 21, the van and the Sentra left at the same time. The Delta van returned to the Terminal 2 secured area of operations. As the van proceeded through a security checkpoint on the way to the Terminal 2 secured area of operations, security surveillance shows that Thorpe was no longer in the vehicle. Nonetheless, minutes later, Thorpe entered Terminal 2 using his security identification.

14. Witnesses identified Okon as a friend and close associate of Thorpe. Okon resides in Springfield Gardens, Queens, New York, with his domestic partner. Okon's domestic partner owns a blue Nissan Sentra. License plate readers on the highway entrances to JFK Airport show Okon's domestic partner's Sentra inbound to JFK Airport at 9:13 a.m. on September 24, 2019, and outbound at 9:16 a.m.

15. On September 29, 2019, law enforcement located the blue Nissan Sentra registered to Okon's domestic partner in Queens, New York. Okon's domestic partner consented to a search of the vehicle. During the search of the blue Nissan Sentra owned by Okon's domestic partner, I found an envelope containing a transfer manifest belonging to the Victim

Security Company and a Delta Air Waybill for the September 24, 2019 Flight 1225, and associated with "Piece 8 of 8." Okon does not now, and has never been, employed by the Victim Security Company, nor was he employed by Delta on September 24, 2019.

16. On Saturday, September 28, 2019, Okon was arrested on probable cause. On Monday, September 30, 2019, Okon was arrested pursuant to a complaint (Dkt. No. 19-MJ-876).

17. On October 24, 2019, a grand jury within the Eastern District of New York returned an indictment against Thorpe and Okon (Dkt. No. 19-492 (MKB)).

18. Based on my training and experience, individuals who coordinate illegal activity typically use phones to plan and coordinate the theft. In particular, in this case, based on my training, experience, review of surveillance and interviews with witnesses, it is my belief that Thorpe called and/or messaged Okon to plan and/or coordinate the pickup of the stolen bag. In addition, individuals who plan conspiracies to commit illegal activities may do so months in advance of the execution of the activities.

19. Also based on my training and experience, historical financial information, such as bank records, checks, credit card bills, account information, and other financial records may evidence a motive to commit a crime and/or the disposition of stolen funds.

20. The Device is currently in the lawful possession of the FBI. The Device was in the possession of Emmanuel Asuquo Okon was seized incident to his arrest on September 28, 2019. While the FBI may already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

21. The Device is currently in my possession within the Eastern District of New York. In my training and experience, I know that the Device has been stored in a manner in

which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

TECHNICAL TERMS

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images.

Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and using computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control

a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

23. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence may be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent

with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that may expose many parts of the Device to human inspection to determine whether it is evidence described by the warrant.

27. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

28. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Robert T. Carasiti
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on October 25, 2019:

HONORABLE VERA M. SCANLON
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is a white Apple iPhone X belonging to Emmanuel Asuquo Okon (the "Device"). The Device is currently in my possession within the Eastern District of New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 371, 659, 981(a)(1)(C), 2 and 3551 et seq. and involve Quincy Thorpe and Emmanuel Asuquo Okon since on or about September 24, 2019, including:

   a. names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), geolocation data, application data, and other electronic media;

   b. evidence of the times the Device was used, to include information recording Emmanuel Asuquo Okon's schedule or travel from September 24, 2019 through September 28, 2019;

   c. passwords, encryption keys, and other access devices that may be necessary to access the Target Device; and

   d. geolocation data from September 24, 2019 through September 28, 2019;

   e. evidence of the formation and execution of a conspiracy to steal, unlawfully take and carry away goods and chattels from John F. Kennedy International Airport in Queens, New York from August 1, 2019 through September 28, 2019;

   f. evidence of the theft, concealment and carrying away of goods and chattels from John F. Kennedy International Airport in Queens, New York from September 24, 2019 through September 28, 2019; and

   g. all bank records, checks, credit card bills, account information, and other financial records from August 1, 2019 through September 28, 2019.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.